Будущая информационная система будет выполнять следующие функции:

1. Учет заказов на выполнение работ;
2. Учет проектных групп;
3. Учет задач по проектным группам студентам;
4. Контроль выполнения проектов;
5. Анализ результатов проектного обучения.

Данные функции представлены на рисунке 2.

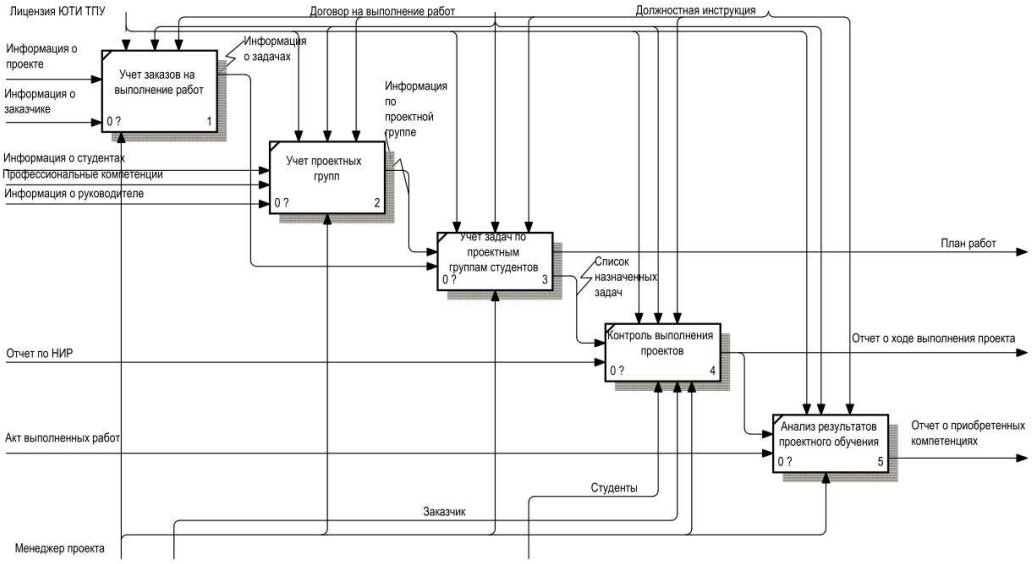

Рис. 2. Функции информационной системы

Пользователями системы будут являться сотрудники отделений, ответственные за проектное обучение студентов. Для сотрудников будет предусмотрен удаленный доступ к системе.

В ходе данной работы были выделены основные цели внедрения информационной системы, ее функции, смоделированы процессы автоматизации. В завершении можно сказать, что данная информационная система позволит улучшить процесс проектного обучения студентов в ЮТИ ТПУ.

Список литературы:

1. Шарипов Ф.В. Технология проектного обучения [Электронный ресурс]. https://irorb.ru/files /magazineIRO/2013november/6.pdf;
2. Н.В. Матяш. Инновационные педагогические технологии. Проектное обучение: учебное пособие для студентов учреждений высшего профессионального образования. М.: Издательский центр «Академия», 2011;

ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ ЕВРОПЕЙСКОГО СОЮЗА: НА ПУТИ К СТРАТЕГИЧЕСКОЙ АВТОНОМИИ

А.К. Паньковская, студент группы 17В81,
научный руководитель: Чеховских К.А., к.и.н., доц.
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26

Аннотация: Кибербезопасность как единая область по-прежнему является новой сферой деятельности общей политики ЕС, в тоже время она широко воспринимается как область растущей важности для глобальной позиции и безопасности Союза. Это развитие политики кибербезопасности ЕС происходит в контексте широко возрастающих усилий, а именно амбиций Европы по увеличению своей стратегической автономии. Для ЕС основной проблемой остается необходимость последова-

тельного и целостного подхода к кибербезопасности, охватывающего все ее аспекты - сетевую и информационную безопасность, киберпреступность и киберзащиту. Новые инициативы, предпринятые на саммитах ЕС в Брюсселе в октябре и декабре 2018 г., направлены на решение этой проблемы.

Целью этой статьи является содействие лучшему пониманию потенциала политики ЕС в области кибербезопасности для формирования будущего европейской безопасности и обороны, а также перспектив развития интернет-пространства в Российской Федерации.

Ключевые слова: кибербезопасность, стратегическая автономия, Европейский союз, киберзащита, киберпреступность, сетевая и информационная безопасность, устойчивость, киберпространство, стратегия, общая политика безопасности и обороны, сдерживание, киберпространство.

Распространение Интернета в последние 25 лет привело к значительному увеличению пользователей глобальной сети, и к началу 2018 года их число превысило 50% мирового населения. Киберпространство является важной сферой деятельности, сотрудничества, а также конкуренции, в которой участвуют как государства, так и негосударственные субъекты. Наряду с положительными моментами за последнее десятилетие, стали выявляться негативные аспекты Интернета, такие как киберпреступность.

В широком смысле киберпространство в целом соответствует ноосфере и в глобальной сети где люди работают, получают знания, общаются друг с другом или просто развлекаются, они в тоже время подвергаются различным угрозам. Нападениям подвергаются личные компьютеры, серверы учреждений, аккаунты, электронная почта, и другие средства коммуникаций. Целью таких нападений или кибератак, является получение важной информации или нанесение различного вида ущерба – финансового, материального, морального или политического.

Масштабы кибератак сегодня представляют собой проблему для национальной безопасности стран и их внутренней стабильности. Развитие ИКТ (информационно-коммуникационных технологий) и Интернета привело к появлению совершенно новых концепций в области международной безопасности, таких как «киберпреступность» и «кибертерроризм».

Актуальность проблемы обусловлено еще и тем, что киберпространство используется в военных целях как оборонительного, так и наступательного характера. Кибератаки часто являются частью сценариев политических и военных кризисов и конфликтов, особенно в контексте комплексного сочетания методов и средств. В связи с этим кибернетический потенциал и возможности становятся важным признаком силы государств в международных отношениях. Следует отметить что, уязвимость или устойчивость к угрозе кибератак, все чаще определяют общее восприятие безопасности и формируют своеобразный рейтинг государств в области кибербезопасности. Этому способствуют ставшие известными примеры сильных кибератак, последствия которых имеют серьезное экономическое значение, нарушают функционирование государственных структур и напрямую влияют на жизнь граждан и их чувство безопасности. По данным исследовательского центра Pew за 2018 г., кибератаки из других стран заняли третье место среди глобальных угроз. Для 56% населения Европейского Союза киберугрозы являются одной из важнейших проблем безопасности. Из-за высокого уровня популяризации Интернета и цифровых услуг в мире, страны ЕС особенно подвержены угрозе кибератак, в контексте которой актуализирована проблема борьба с дезинформацией в интернете.

Для Европейского Союза широко понимаемая политика кибербезопасности приобрела всеобъемлющее стратегическое измерение довольно поздно. Фактически это произошло только после принятия документа о стратегии кибербезопасности ЕС в 2013 г. Однако с тех пор началось интенсивное развитие политики ЕС в отношении киберпространства во всех его измерениях: цифровая экономика, сетевая и информационная безопасность, борьба с киберпреступностью, а также общая внешняя политика и политика безопасности и киберзащита. Это также относится к сотрудничеству ЕС с другими субъектами безопасности, такими как НАТО. Эволюция подхода к этому вопросу особенно заметна в Глобальной стратегии внешней политики и политики безопасности Европейского Союза, в которой кибербезопасность упоминается в качестве неотъемлемых элементов безопасности Союза.

Признавая, что информационные технологии стали основой для функционирования и благополучия европейских обществ, ЕС сделал кибербезопасность одним из своих основных приоритетов в области безопасности. В то же время недавние события вокруг и внутри ЕС, такие как агрессия США по отношению к Росси, Brexit и неопределенность в отношении будущего трансатлантических отношений после избрания Дональда Трампа на пост президента Соединенных Штатов, усилили дебаты об укреплении независимости ЕС в сфере безопасности и обороны, а также расширении сферы стратегической автономии. Нет недостатка в том, что политика кибербезопасности как относительно

новая область, не обремененная политическими событиями, может стать зародышем и специфическим испытательным полигоном для стратегической автономии ЕС.

Политика ЕС в области кибербезопасности, несмотря на явный прогресс, достигнутый в последние годы, все еще не является полностью понятной, и ей не хватает необходимой согласованности. Это проявляется как на регулятивном, так и на институциональном уровнях. Стремление ЕС к достижению стратегической автономии в киберпространстве не имеет достаточно прочной основы и в значительной степени остается на уровне амбиций. В традиционном измерении (так называемая жесткая сила) видение полной стратегической автономии, связанной с наличием собственных возможностей киберзащиты, остается не реализовано. Государства-члены признают необходимость укрепления своих ресурсов, но не хотят делиться своими возможностями. Потенциал отдельных государств в области кибербезопасности также очень разнообразен, и между группой лидеров и остальными существуют различия. Необходимость поддерживать тесное, институционализированное сотрудничество Соединенного Королевства с ЕС в области кибербезопасности отмечается как в Лондоне, так и в Брюсселе. В области возможностей киберзащиты европейские государства предпочитают сотрудничество и разделение задач между ЕС и НАТО, в то время как действия ЕС рассматриваются в значительной степени взаимодополняемо. Стоит отметить, что сотрудничество НАТО-ЕС в области киберзащиты развивается практически без перерыва и до сих пор избегало политизации. Осуществление Совместной декларации НАТО-ЕС, подписанной в июне 2016 года в кулуарах саммита альянса в Варшаве, идет гармонично в области кибербезопасности и киберзащиты, о чем свидетельствует последний доклад о ее реализации.

ЕС направлен в большей степени на так называемую мягкую безопасность: усиление внешнего измерения политики ЕС в области кибербезопасности, повышение устойчивости сетей и систем ИКТ к киберугрозам, разработка возможностей и инструментов для реагирования на кибератаки, эффективное сотрудничество в борьбе с киберпреступностью, продвижение стандартов и ценностей в киберпространстве. Прогресс в этих областях будет определять потенциал ЕС в этой области и его положение на мировой арене. Однако в ближайшие годы потребуется предпринять осознанные и скоординированные действия, поддержанные соответствующим уровнем финансирования. Осуществление этого нового подхода опубликовано в сентябре 2017 года, так называемый пакет кибербезопасности, содержащий множество различных предложений. Некоторые условия для оптимизации представлены в проекте многолетней финансовой структуры на 2021-2027 годы, обнародованной 2 мая 2018 года. Он предполагает значительно увеличить средства в области кибербезопасности, в частности в рамках программы исследований и инноваций, стратегической инвестиционной программы «Цифровая Европа» и «Европейского оборонного фонда». Только реализация этих планов создаст прочную основу для построения стратегической автономии ЕС. Европейский Союз в силу своих экономических интересов, глобальных амбиций и направлений угроз безопасности должен разработать и реализовать надежную политику кибербезопасности, которая будет основываться на соответствующих инструментах и функциональных институтах. Европа не может отказаться от своей активной политики в киберпространстве, которое становится еще одной областью стратегической конкуренции в глобальном масштабе. Будет ли она двигаться в направлении большей стратегической автономии, зависит как от потенциала ЕС, так и от политической воли государств-членов. Европа должна быть заинтересована в самом полном участии в разработке политики кибербезопасности ЕС. Трансграничный характер киберугроз приводит к тому, что устойчивость ЕС в этом вопросе напрямую влияет на ее национальную безопасность. Текущее направление развития потенциала ЕС в этом вопросе, и особенно тесное сотрудничество с НАТО, дают шансы избежать сложных политических дилемм. В то же время область широко понимаемой кибербезопасности в настоящее время является важной областью сближения интересов Европы и США, особенно в условиях растущей конкуренции основных мировых игроков за влияние на форму киберпространства. Все евроатлантическое сообщество заинтересовано в том, чтобы не допустить фрагментации киберпространства и сохранить его открытый, свободный и универсальный характер.

Список литературы:

1. Кавелти М.Д., Европейская кибер-держава, «Европейская политика и общество» 2018, том 19, № 3, URL: https://doi.org/10.1080/23745118.2018.1430718. (дата обращения: 27.02.2019).

2. Данилюк П., Стратегическая культура Европейского Союза. Нормативный подход, 2015, т. 9, № 2. (дата обращения: 27.02.2019).
3. Исследовательский центр Pew, август 2017 г., URL: http://www.pewglobal.org/2017/08/01/globally-people-point-to--isis-and-climate-change-as-leading-security-threats/ (дата обращения: 27.02.2019).

ПРИМЕРЫ МОДЕЛЕЙ И ДАННЫЕ ДЛЯ АЛГОРИТМА ПО ОЦЕНКЕ УРОВНЯ СФОРМИРОВАННОСТИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ КОМПЕТЕНЦИЙ

Н.А.Кузнецова, студент группы 17В60, научный руководитель: Молнина Е.В. Ст. преподаватель
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-mail: nak1911@yandex.ru

Аннотация: в статье приводятся модели оценки сформированности информационно-коммуникационных компетенций, а также примеры входной и выходной информации для разрабатываемого в рамках УИРС алгоритма оценки.

Ключевые слова: информационная система, информационно-коммуникационная компетентность, анализ, оценка компетенций, ФГОС, входная и выходная информация, модель оценки компетенций.

Информатизация является одной из самых важных характеристик мира на данный момент. Все области деятельности человека тесно связаны с такими процессами, как поступление, обработка, преобразование и передача данных для их использования в различных сферах жизни и деятельности человека. Увеличение объема данных приводит к тому, что люди стараются дополнить свою жизнь тем, что им поможет в этом разобраться. Помощником в данном случае являются информационно-коммуникационные технологии. Все это прямо влияет на развитие информатизации общества.

Одной из главных частей информатизации можно считать информатизацию образования. Это означает, что происходит преобразование процессов образования с использованием ИКТ.

Федеральные Государственные образовательные стандарты предполагают, что студент будет осваивать определенные компетенции, а именно профессиональные и общеобразовательные, пока обучается на бакалавра в университете. В подготовке таких специалистов одну из значимых ролей играют информационно-коммуникационные компетенции.

Информационно-коммуникационная компетентность является одной из главных частей профессиональной компетентности.

Ранее в рамках научной деятельности в институте студентом Гнедашом Д.В. была создана «Информационная система оценки и анализа уровня сформированности компетенций студентов направления Прикладная информатика ЮТИ ТПУ», которая в последствие стала темой его выпускной квалификационной работы. На ее основе в рамках данной работы и будет создаваться новый алгоритм оценки сформированности информационно-коммуникационных компетенций.

Созданная система выполняет следующие функции: Формирование «ФОС»; Оценка сформированности компетенций; Анализ сформированности компетенций.

Оценка компетенций в данной системе происходит с учетом результатов тестов в среде Moodle Томского политехнического университета. После чего эти результаты используются для оценки уровня сформированности компетенций студентов с помощью документа «Оценочное мероприятие» [1].

Для добавления в созданную информационную систему нового алгоритма оценки компетенций необходимо рассмотреть модели оценки информационно-коммуникационных компетенций, наиболее подходящих под задачи проекта.

Например, модель информационно-коммуникационной компетентности по Андреевой предполагает определенные действия, при которых полученные баллы по дисциплине сравниваются с другими дисциплинами и преобразовываются в оценку от 1 до 5, как это показано в таблице 1 [2].